Kiteworks

CASE STUDY

INDUSTRIAL MANUFACTURING • IP PROTECTION • DATA POLICY ENGINE

Protecting Intellectual Property at the Edge of the Supply Chain

A global advanced energy technology manufacturer deployed Kiteworks with a two-tier executive approval workflow and MIP-integrated Data Policy Engine to govern outbound transfer of highly restricted technical data to supply chain partners -- without disrupting existing operations.

DATA POLICY ENGINE (ABAC) | MIP LABEL INTEGRATION | APPROVAL WORKFLOWS | SFTP/MFT | OKTA CONDITIONAL ACCESS | SECURE EMAIL

THE CHALLENGE

Proprietary data leaving the organization with no policy enforcement at the edge

What wasn't working

The company had invested in Microsoft Information Protection (MIP) sensitivity labels to classify data internally -- Highly Restricted, Confidential, Internal -- but those classifications had no enforcement power the moment a file crossed the organizational boundary. A file labeled Highly Restricted could leave through a legacy file-transfer platform just as easily as one labeled Public. There was no mechanism to require human authorization before sensitive technical specifications, firmware, or process data reached an external partner, and no reliable audit trail for compliance teams. At the same time, a key supply chain partner required automated SFTP transfers -- a capability the legacy platform offered only without content policy controls.

What Kiteworks delivered

Kiteworks secure data exchange extended the company's existing MIP classification framework to every outbound transfer channel. The Data Policy Engine (DPE) reads MIP sensitivity labels at runtime and applies the appropriate policy: Confidential files transfer automatically under standard controls; Highly Restricted files trigger a two-stage executive approval chain before any data moves. SFTP was configured with profile-based access controls, enforcing the same DPE policies for automated partner transfers. Okta conditional access restricts Kiteworks authentication to managed corporate devices, closing the personal-device exposure gap that had concerned the security team.

> Your innovative approach to data classification with MIP is setting a new standard. Your successful go-live in early April 2026 is a significant milestone that reflects your team's dedication and collaborative spirit.

KITEWORKS CUSTOMER SUCCESS
ON GO-LIVE, APRIL 2026

HOW IT WORKS

Two-tier approval workflow for restricted IP -- enforced at the policy layer, not by procedure

When a user attempts to share a file classified as Highly Restricted, the Data Policy Engine intercepts the transfer and triggers a structured authorization chain. No file moves until both stages are cleared. Confidential and lower classifications pass through automatically under standard access controls — no user friction for routine transfers.

TRIGGER
User initiates transfer
File, folder share, email, or SFTP upload attempted

>

DPE READS LABEL
MIP label evaluated
Highly Restricted triggers approval chain; Confidential passes automatically

>

STAGE 1
VP Authorization
Business unit VP notified via Outlook; must explicitly approve

>

STAGE 2
Legal Review
Legal team reviews and confirms; full audit trail on approval and denial reasons

>

RELEASE
Transfer completes
Data delivered to recipient; event logged to audit trail

Go-live required provisioning 38 VP and legal accounts with executive profiles and sign-off from the information security steering committee. Testing with actual VP and legal approvers validated notification routing, audit log capture, and denial-reason handling before any production traffic was enabled.

PLATFORM CAPABILITIES

One governed exchange perimeter -- across every data movement channel

SFTP with DPE enforcement

Two SFTP profiles -- restricted and standard -- give the security team granular control over which users can access which data tiers. SSH key authentication enforced for external partners. OPE policies apply identically over SFTP as over the web UI, eliminating the policy gap the legacy platform left open.

Okta conditional access

Rather than IP whitelisting -- impractical across the company's many global manufacturing sites -- Okta conditional access policies restrict Kiteworks authentication to managed corporate devices. Internal users are fully covered; external partners operate under a separate policy appropriate to their access level.

MIP label synchronization

Kiteworks reads MIP label GUIDs embedded in files and surfaces label names in the UI, distinguishing between internal AEI labels and external labels from acquired entities. OPE acts on the correct label set without confusion -- a critical requirement given the company's acquisition history and mixed label environments.

USE CASES

Four governed exchange patterns -- all enforced by the same policy layer

1

Restricted IP transfer to supply chain partners

Technical specifications, firmware, and process data shared with strategic manufacturing partners under two-tier VP + legal approval. DPE blocks Highly Restricted files until both stages clear; Confidential transfers proceed automatically.

2

Automated SFTP for partner data exchange

SFTP-based automated transfers to a key supply chain partner, with DPE enforcement ensuring restricted data cannot transit the automated channel without policy clearance. SSH key authentication and profile-based access controls applied throughout.

3

Legacy platform migration

Full decommission of the legacy LiquidFiles system. High-usage customers were contacted directly for transition; an internal SharePoint training site with video tutorials and self-service request workflows enabled a selfdirected migration with no centralized retraining sessions.

4

Factory floor device access

Field technicians using shared devices on the factory floor upload hardware images through shared accounts. SSH key management options within Kiteworks SFTP profiles accommodate this use case while keeping broader session and device policy intact for all other users.

RESULTS

Policy-enforced IP protection -- from go-live to executive expansion

38
VP and legal accounts provisioned for approval workflow at go-live

April 2026
On-schedule go-live with no disruption to existing file-transfer operations

0
Retraining sessions required -- self-service SharePoint training site covered all users

100%
DPE coverage across file sharing, email, SFTP, and MFT -- every channel, one policy

Needs addressed

- ✓ Policy-enforced IP protection at every outbound transfer point
- ✓ MIP sensitivity label enforcement extended to the partner edge
- ✓ Two-tier VP + legal approval workflow for Highly Restricted transfers
- ✓ Automated SFTP partner exchange with DPE enforcement intact
- ✓ Device-level access control via Okta conditional access
- ✓ Full legacy platform decommission with zero retraining sessions

Kiteworks capabilities deployed

- ✓ Data Policy Engine (ABAC) with MIP sensitivity label integration
- ✓ Custom approval workflows — VP authorization + legal review
- ✓ SFTP with profile-based access control for internal users and external partners
- ✓ Okta conditional access integration for managed-device enforcement
- ✓ Secure email and silo folder architecture for classification-level separation
- ✓ Full audit trail on every approval decision — approval, denial, and denial reason